TechNote

GMS | Troubleshooting Security Appliance Acquisition in GMS

Introduction

This Technical Note provides instructions for troubleshooting the most common problems you may encounter when acquiring SonicWALL security appliances for the SonicWALL Global Management System (GMS), or when a working SonicWALL security appliance stops sending heartbeat messages to GMS (changes from blue status to a prolonged red state for longer than expected). The most common and easily diagnosed causes for these problems (such as the offline unit is offline, or experiencing hardware failure, or has no interruption of Internet access) are not covered in this Technical Note.

GMS version 2.8 was used for the development of this Technical Note. However, most procedures can be accomplished executed in any GMS version.

This Technical Note discusses the three Problem Scenarios with the different management methods that can be used in GMS, and the different troubleshooting methods used for each. At the end of each management scenario, you will find each Problem Scenario concludes with checklist of procedures to that will help troubleshoot and solve the problem. Most of the items in these checklists refer to more detailed instruction found in this are detailed in the Troubleshooting Techniques section of this Technical Note's Appendix.

You should be able to solve most GMS acquiring problems if you follow these procedures.

Troubleshooting Scenarios

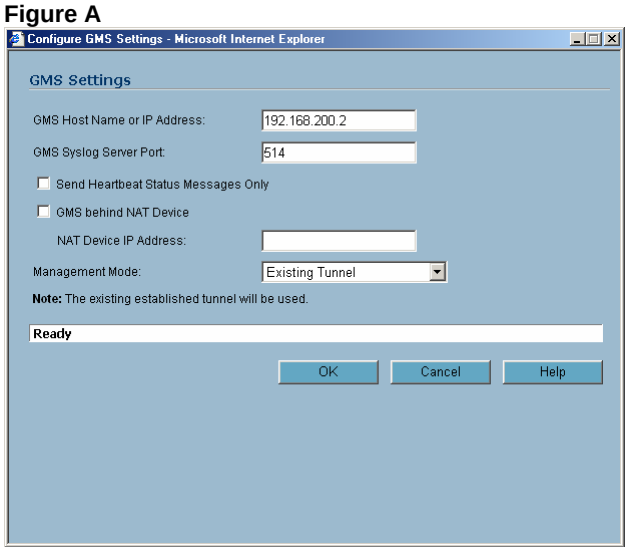
GMS is able to communicate with and acquire security Appliances using different management methods for Existing Tunnels, IPSec Management Tunnels, and HTTPS

Existing Tunnel

In general, you should use this management method if the security Appliance is able to reach the GMS local network. This can be accomplished via a static route, a VPN tunnel, or direct access if the box is on the same subnet as the GMS installation.

Figure A shows the **Configure GMS Settings** with the correct settings for an Existing Tunnel. The IP address 192.168.200.2 is the GMS agent/scheduler that will manage the security Appliance.

Figure A



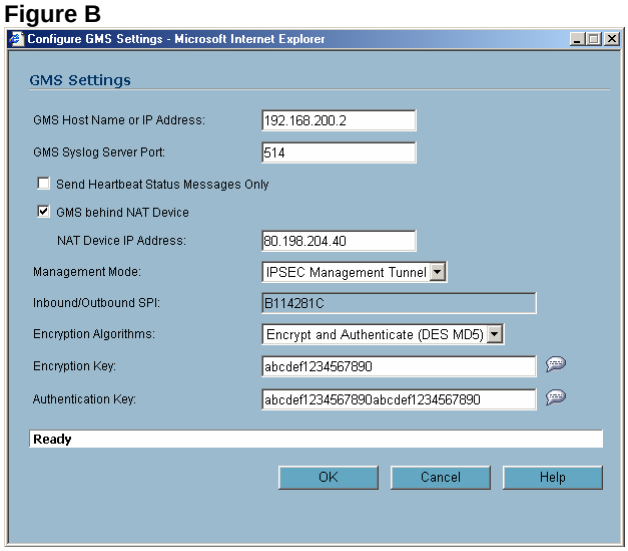
If you are having a problem acquiring a security Appliance using this method, use the following checklist to troubleshoot the problem:

- Is the security Appliance sending any heartbeat messages to the GMS? (Troubleshooting Technique 1)
- Are you able to ping the GMS host? (Troubleshooting Technique 3)
- Are the options selected correctly on the security Appliance and in the GMS console? (Troubleshooting Technique 4)
- Is the GMS agent able to login to the unit? (Troubleshooting Technique 5)
- Is the time correctly set on the unit and on the GMS agent? (Troubleshooting Technique 7)
- Are you able to login to the unit from the GMS agent by using the LAN IP?
- Other unexplained problems see (Troubleshooting Technique 8) and Release Notes.

IPSec Management Tunnel

Configure GMS Settings in Figure B shows the correct settings for this method. The IP address 192.168.200.2 is the GMS AGENT/scheduler that will manage the security Appliance. The IP address 80.198.204.40 is the IP address of the GMS gateway.

Figure B



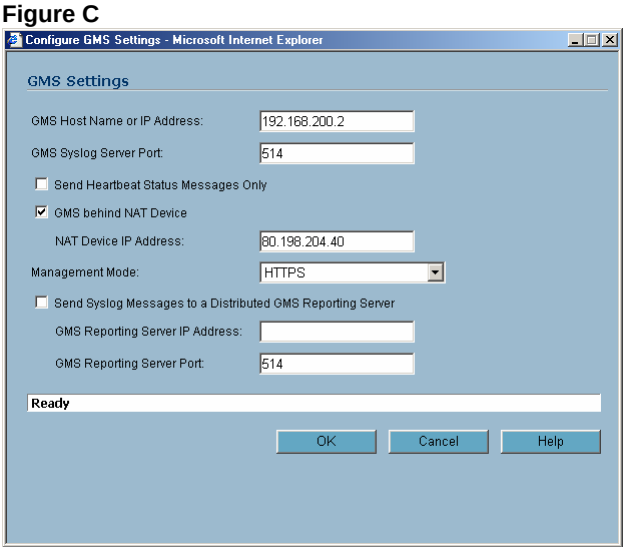
If you are having a problem acquiring a security Appliance using this method, use the following checklist to troubleshoot the problem:

- Is the security Appliance sending any heartbeat messages to the GMS? (Troubleshooting Technique 1)
- Are you able to ping the GMS host? (Troubleshooting Technique 3)
- Are the options selected correct on the security Appliance and in GMS? (Troubleshooting Technique 4)
- Is the GMS agent able to login to the unit? (Troubleshooting Technique 5)
- Is GMS able to create a correct SA on the Gateway? (Troubleshooting Technique 6)
- Is the time correctly set on the unit and on the GMS agent? (Troubleshooting Technique 7)
- Are you able to login to the unit from the GMS agent by using the WAN IP?
- Other unexplained problems see (Troubleshooting Technique 8) and Release Notes.

HTTPS

Configure GMS Settings in Figure C shows the correct settings for this method. The IP address 192.168.200.2 is the GMS agent/scheduler that will manage the security appliance. The IP address 80.198.204.40 is the IP address of the GMS gateway.

Figure C



If you are having a problem acquiring a security Appliance using this method, use the following checklist to troubleshoot the problem:

- Is the security Appliance sending any heartbeat messages to the GMS? (Troubleshooting Technique 1)
- Are the options selected correct on the security Appliance and in GMS? (Troubleshooting Technique 4)
- Is the GMS agent able to login to the unit? (Troubleshooting Technique 5)
- Are you able to login to the unit from the GMS agent by using HTTPS and the units WAN IP?
- Is the time correctly set on the unit and on the GMS agent? (Troubleshooting Technique 7)
- Have you created a NAT policy on the GMS agent allowing SYSLOG to NAT to the Agent?
- Other unexplained problems see (Troubleshooting Technique 8) and Release Notes

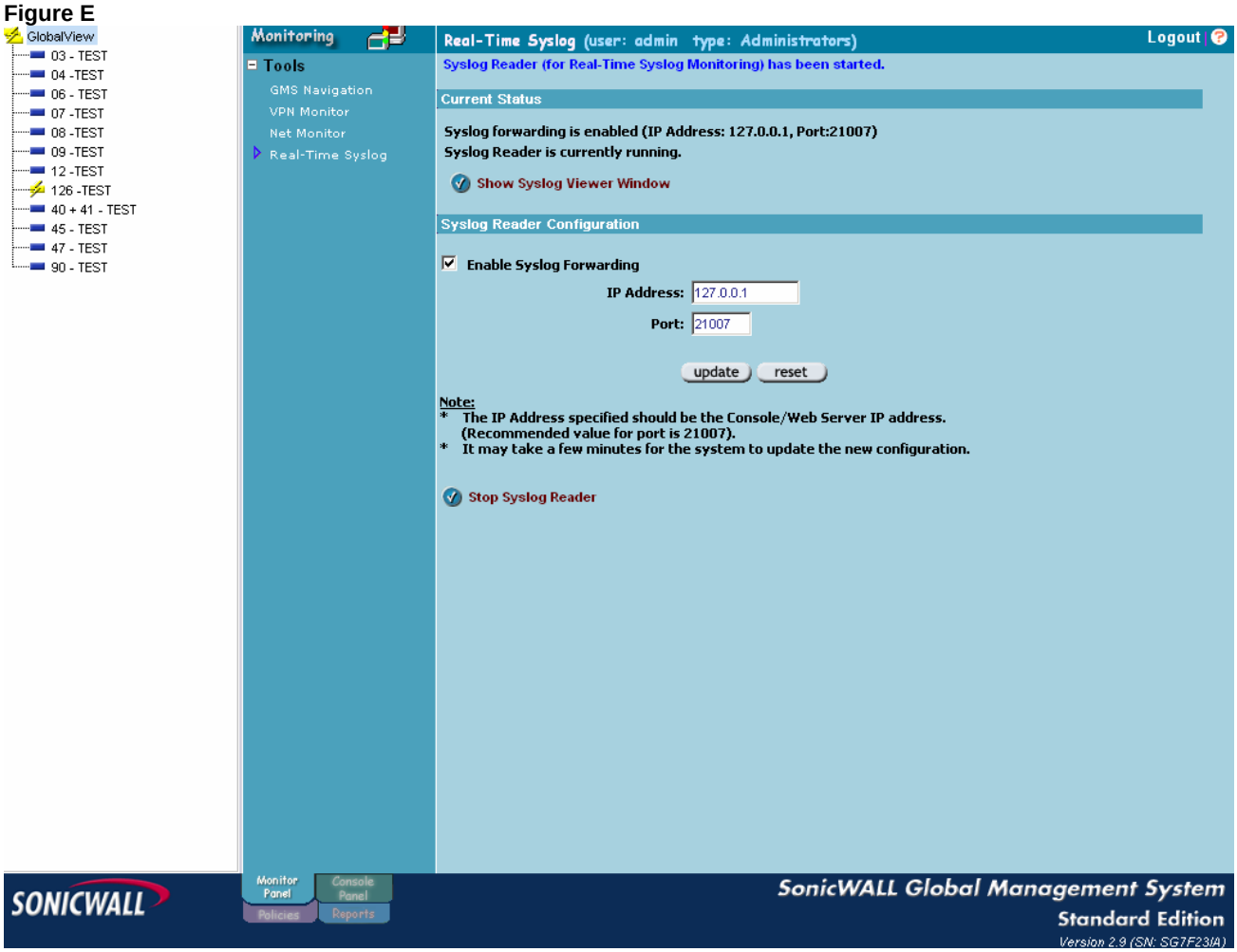
Troubleshooting Techniques within GMS

Troubleshooting Technique 1: How to see a heartbeat message using real-time syslog monitor

In GMS 2.8, the real-time syslog monitor in the monitor panel can be used for troubleshooting tasks. In this scenario, it is used to verify if GMS receives any heartbeat messages from a specific unit.

First, log into GMS, then select the Monitor panel.
If the real-time syslog monitor has not been started, start it. Click **show syslog viewer window**.

Figure E

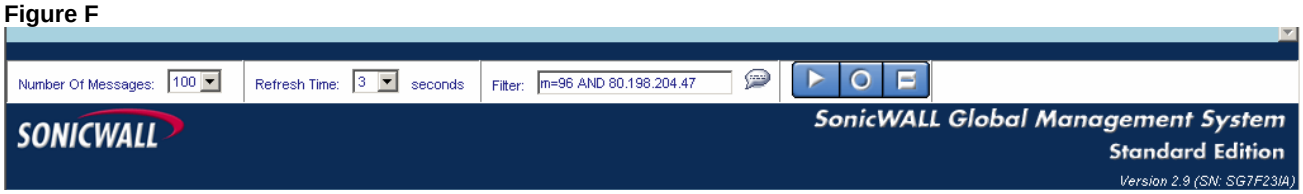


Next, enter in the filter box “m=96 AND WAN_IP” like the figure below shows. If the security appliance is able to send heartbeat messages you will see a message that should look like this:

```
<128id=firewall sn=006B1060228 mgmtip=80.198.204.47 time=”2005-01-07 10:51:04 UTC
fw=80.108.204.47 m=96 n=5816 i=60 lic=2 pt=80.443 usestandbysa=0 dyn=n.n
fwlan=192.168.47.1
```

Please note that a heartbeat message is only sent once every 60 seconds by default.

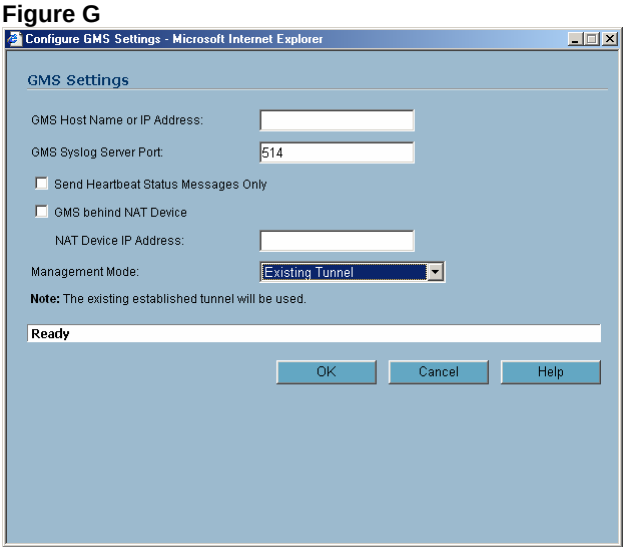
Figure F



Troubleshooting Technique 2: Explanation of settings in the “Configure GMS Settings” window located in the security appliance management interface

General management options:

Figure G



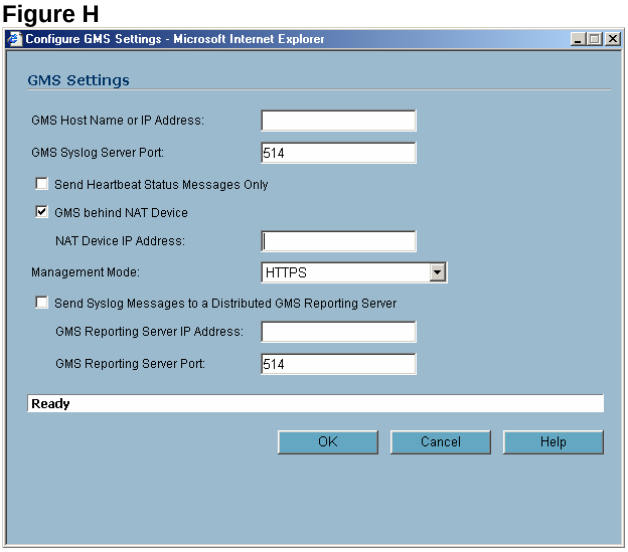
GMS Host Name or IP Address: The physical IP address of the GMS agent/scheduler that will acquire the security appliance.
GSM Syslog Server Port: The syslog port (default: 514).

Send Heartbeat Status Messages Only: This option should be used if you do not need the data to generate reports in GMS. When you check this setting, the unit will only send heartbeat (m=96) messages that tell GMS that the unit is alive.

GMS behind NAT Device: This option should be checked if the GMS agent/scheduler is behind a SonicWALL (GMS gateway). This option is not checked when using existing tunnels method. The IP address inserted should be the WAN IP of the gateway or the IP that the VPN is terminated upon.

HTTPS management specific options:

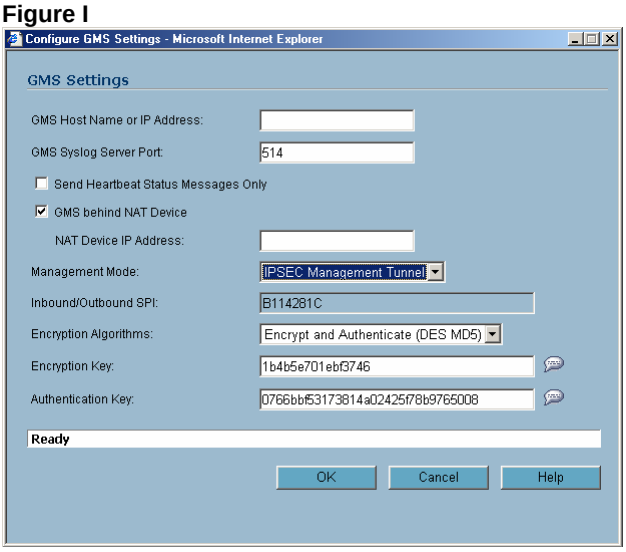
Figure H



Send Syslog Messages to a Distributed GMS Reporting Server: By checking this you will be able to send the syslog to another server if it is not the default agent/scheduler that will collect the syslog heartbeat (m=96) messages which tell GMS that the unit is alive.

IPSEC management specific options:

Figure I



Inbound/Outbound SPI: This number represents the Serial number of the unit, minus the first 4 digits.

Encryption Algorithms: Select the encryption and authentication method for the management tunnel.

Encryption key: The encryption key used for the management method.

Authentication key: The authentication key used for the management method.

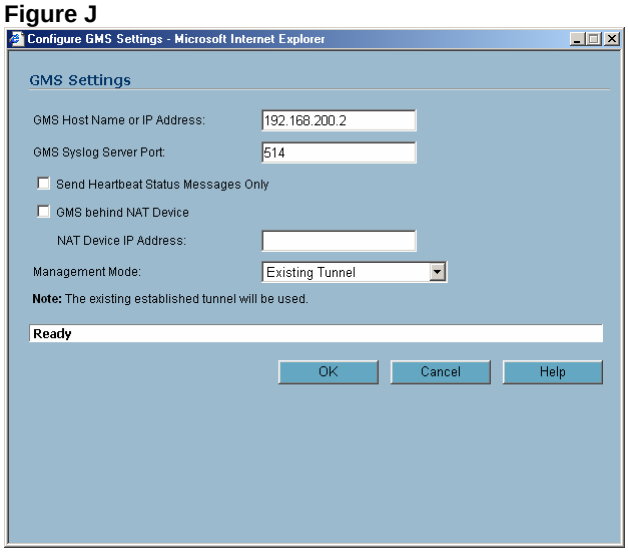
Troubleshooting Technique 3: How to check if a box is acquired by GMS using ping

If you are on site where a security appliance is deployed and what to check if the unit has been acquired by GMS, login into the box, locate the diagnostic tools in the GUI, select PING, and try ping the GMS Agent/Scheduler. If you get a response the tunnel or access are OK and the box should come online within a few minutes. This method only works if you are using IPSEC or existing management tunnels.

Troubleshooting Technique 4: Management method configurations on the security Appliance and in GMS

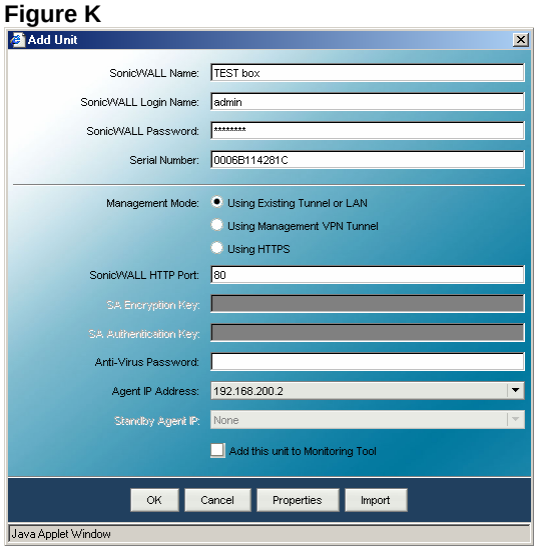
If the settings in the following screens are unclear, refer to Troubleshooting Technique: 2 for definitions.
GMS screen for appliance configured using **Existing Tunnels**.

Figure J



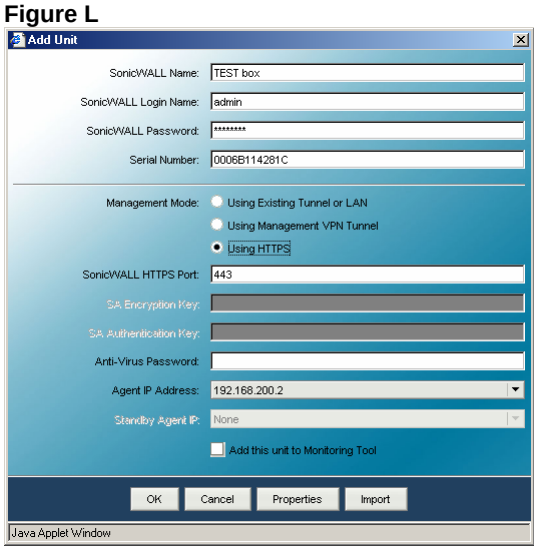
Appliance screen for appliance configured using **Existing Tunnels**.

Figure K



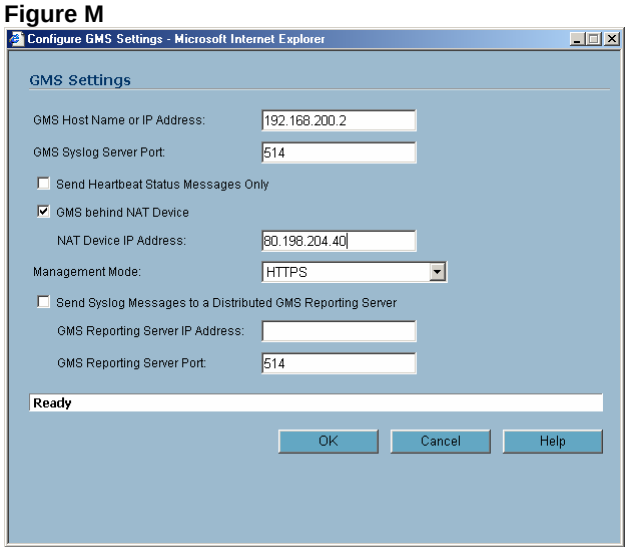
GMS screen for appliance configured using **HTTPS.**

Figure L



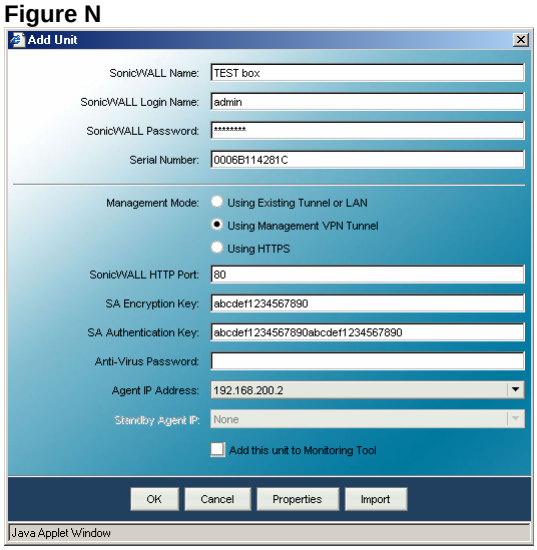
Appliance screen for appliance configured using **HTTPS**.

Figure M



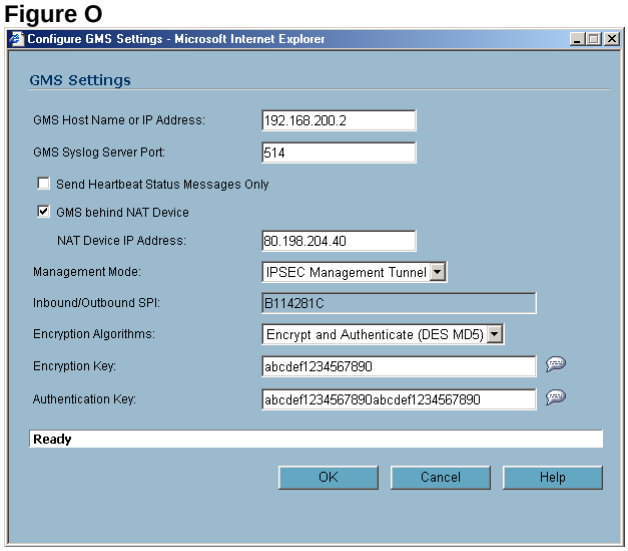
GMS screen for appliance configured using IPSEC management tunnel.

Figure N



Appliance screen for appliance configured using **IPSEC management tunnel**.

Figure O



Troubleshooting Technique 5: The Scheduler log file

For troubleshooting, the Scheduler log file is an important tool. In this log file, GMS logs every action that the Agent/Scheduler performs. The list below shows some of the useful information the log file contains, which are useful for troubleshooting acquiring units in GMS:

- GMS able to login to the GMS gateway.
- Task execution.
- Successful communication with the database.
- Login to units.

The StdScheduler file can be located on the following path *C:\SGMS2\Logs\StdScheduler0.log* (the number could be anywhere from 0 to n (where n is the number of max log files allowed configured in sgmsConfig.xml. Pick the log with the most recent timestamp. As an example, here is sample log file entry if the password entered into the GMS 'Add Unit' dialogue box is not the same as on the security appliance (log cut-out from the stdscheduler log).

```
[Scheduler/executeTask()]: scheduler SGMS 1 (id 1): method: Firewall.login
error: failure response http://x.x.x.x:80/auth3.cgi
```

On the unit, the entry looks like this:

UTC 01/10/2005 08:06:52.000	Alert	Authenticated Access	Administrator login denied due to bad credentials	192.168.200.2 , 3298, WAN	192.168.3.1, 80, LAN

This is how the entry should look, if GMS is able to successfully login and out of a unit again:

UTC 01/10/2005 08:12:5528	Info	Authenticated Access	Administrator logged out	192.168.200.2 , 0, WAN (admin)	x.x.x.x, 80, WAN

Troubleshooting Technique 6: Management tunnels on the GMS gateway

When you are using IPSEC Management tunnels, GMS will automatically create a tunnel on the GMS gateway according to the data that you have entered in the GMS 'Add Unit' dialogue box. First GMS will login to the GMS gateway and create an SA, you will see the following message in the StdScheduler log file if GMS is able to login and successfully create SA's on the gateway.

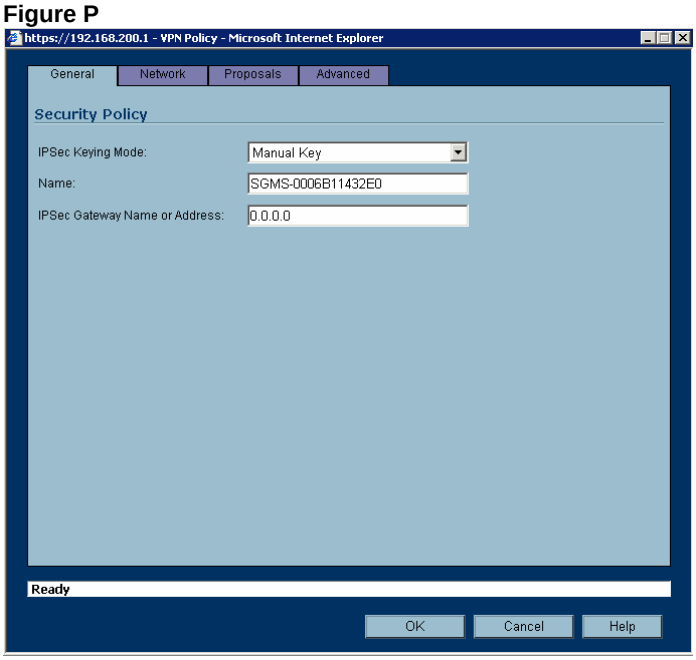
```
[Scheduler/addOrChangeSa()]: scheduler SGMS 1 (id 1): created SA for firewall
```

If GMS is able to create the SA, you should be able to locate it under the VPN summary on the GMS gateway.

```
SGMS-0006B11432E0          0.0.0.0                    ESP DES HMAC MD5
```

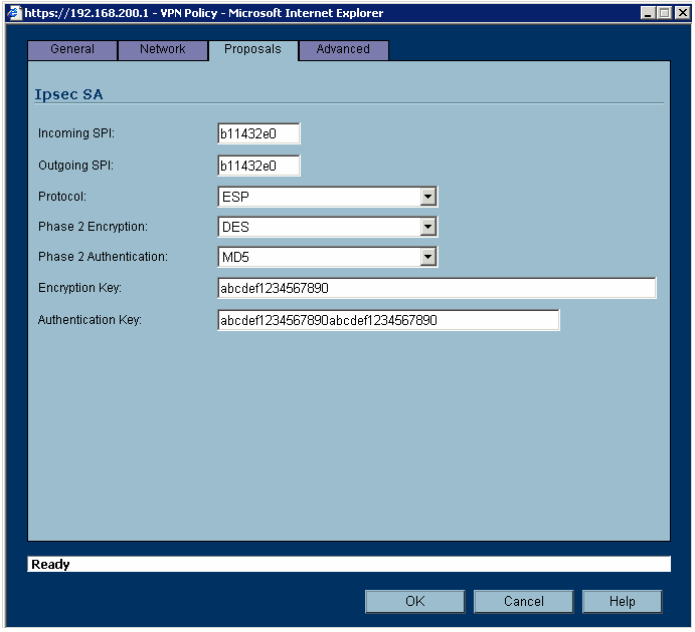
Here are some of the things to check. On the **General** page, the Name of the SA, Is always 'SGMS-<serial number>'. See Figure P for an example. The SA name and the Serial number of the unit added to GMS management should correspond.

Figure P



On the **Proposals** tab, the SA details should correspond to the options that you have previously set on the box (see Troubleshooting Technique 4).

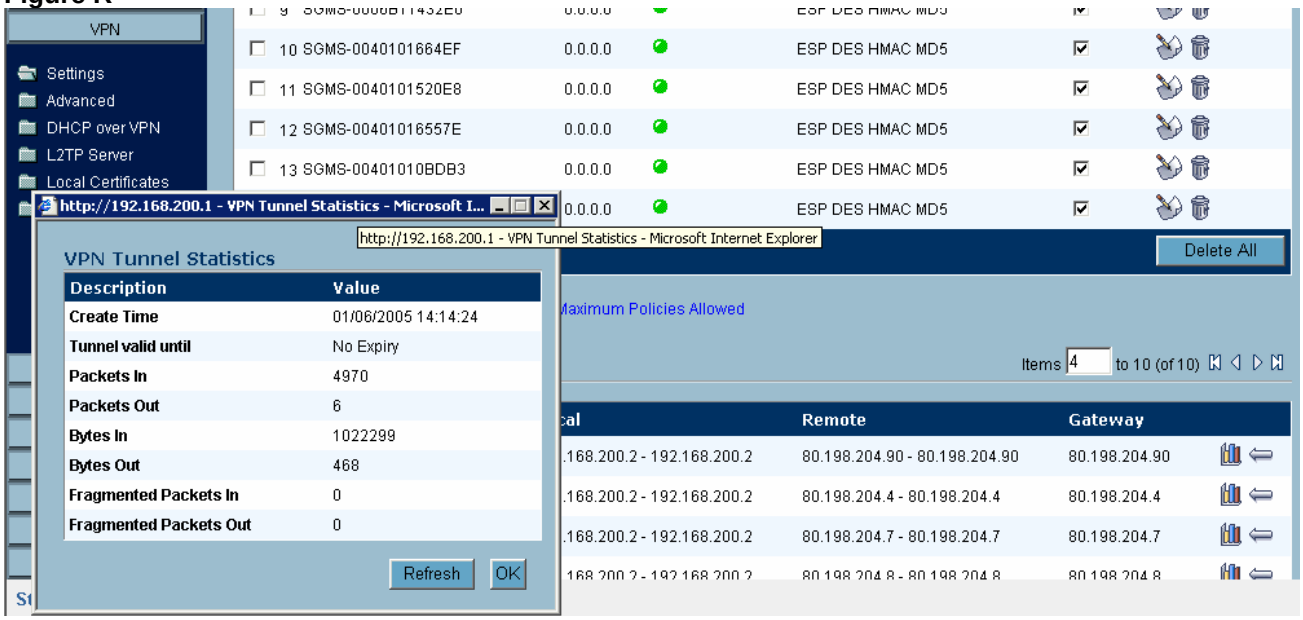
Figure Q



If everything is configured correctly, you should see the security appliance start to negotiate the tunnel. Please note this tunnel is an 'Aggressive Mode' tunnel. To verify the configuration, you should see a green indicator for the SA, and you should be able to see traffic going in both directions on the VPN Tunnel Statistic for the SA in the VPN summary page

You may notice initially that traffic is unidirectional, from the appliance to GMS. After GMS has accepted the initial connection, data transfer will be bi-directional (starting with registration tasks etc).

Figure R



Troubleshooting Technique 7: Time and date in GMS

Configuring the correct time and date in GMS and on the units is **very** important. GMS will discard any syslog/heartbeat message if there is more than 2 hours difference between the agent and the unit. If a unit appears to be configured correctly but is still not acquired by GMS, do a simple time check may solve this issue.

Troubleshooting Technique 8: Other problems and tricks

If you exhaust all the troubleshooting tricks in this Technical Note and still cannot solve the problem, below are some tips that may help.

- Select a different management method.
- Disabling GMS management, rebooting the unit and enabling it again.
- Firmware upgrading.
- Resetting the unit and configure it again.

If none of these suggestions work, you should collect all the documentation that you can from the unit and from GMS. Below is the information that SonicWALL support will request.

- The Technical Support Report of the SGMS Gateway, also a TSR of the unit you have problem with .Go to **Tools > Diagnostic** and select **Technical Support Report** at the drop down menu, tick every option and press save.
- Compress the log folder <"C:\SGMS2\LOGS" by default> within one file. Use only files that end with .txt or .log).
- Include the SGMSCONFIG.XML file from the root of the C:\ drive (where the SGMS software is installed upon)
- Optionally provide a screenshot of the error message which is occurring with your SGMS software.
- Attach the TSR(s), Compressed Log folder file and the SGMS config file onto this Service Request at your mysonicwall account.
- Provide console-access to the SGMS system (VNC, TSE). If this is possible, please also post the connection details in this SR."

Document Created: 01/26/2005
Last Updated: 06/11/08
Version 1.1